Remarks

I. Status of the Application

Claims 1-67 are pending in the application. Claims 1-47 have been rejected. Claims 48-67 have been added.

II. Claim Rejections - 35 U.S.C. § 102

Claims 1-47 were rejected under 35 U.S.C. 102(e) as being allegedly anticipated by US Patent 6,658,004 ("Kadansky"). The rejection is respectfully traversed.

In an example of embodiments of the invention, a method is provided to protect against unauthorized access to stored data. This objective is accomplished by periodically verifying the identity of a client computer from which data processing requests are received. A storage server responsible for managing data processing requests establishes a communications session and confirms a client computer's initial authorization to access the stored data. Data processing requests received from the client computer are serviced as long as the client computer retains its authorization.

At periodic intervals throughout the communication session, the client computer generates "heartbeat" messages containing information verifying its identity, and transmits these heartbeat messages to the storage server. Each time the storage server receives a heartbeat message from the client computer, the storage server confirms the verification information contained therein to determine the identity of the client computer. If the verification information contained in the message is confirmed, the heartbeat message is determined to be a valid message. The storage server additionally tracks the receipt of the heartbeat messages against a schedule defining multiple intervals of a predetermined length. As long as the storage server receives a valid heartbeat message from the client computer during each interval, the storage server continues to service data processing requests received from the client computer. If an interval occurs in which no valid heartbeat message is received, the storage server revokes the client computer's authorization to access the stored data, and ceases to service data processing requests received from the client computer.

Accordingly, claim 1 requires "establishing an authentication handshake with the second computer," "periodically sending messages to the second computer," and "wherein the second computer services the requests if the messages are valid and are received within a predetermined time interval."

Kadansky discloses a method for classifying messages sent among clients in a communication network in order to reduce the wasteful allocation of processing resources to the processing of duplicate, replayed or stale messages (col. 3, lines 11-19). The method disclosed in Kadansky is used in a communication network such as a chat room, where messages (such as email messages) are sent and received among large numbers of clients in a session. A session moderator broadcasts a "beacon message" to multiple clients in a network that send messages among themselves to establish a common time frame for all the clients (col. 2, lines 1-3). Each beacon message contains a sequence number. Subsequently, when one of the clients sends a data message to another client, the sequence number from the most recently received beacon message is included in the data message (col. 5, lines 40-52). The receiving client extracts the sequence number from the message and determines whether or not to discard the message based on the sequence number (col. 6, lines 19-32). For example, if the sequence number in a data message is sufficiently "old," a duplicate, or a replay the message may be discarded (col. 3, lines 11-15).

However, nowhere does Kadansky teach or suggest the combination of limitations recited in claim 1. The "computer" recited in claim 1 may be read onto either the "session moderator 14" or onto one of the "clients" in the network disclosed in Kadansky. However, under neither interpretation does the reference teach or suggest the claimed combination. First, if "the computer" recited in claim 1 is interpreted to be the session moderator and the claimed "second computer" to be one of the clients in the network, there are no "requests from the computer [session moderator] to a second computer [client]." Nor is there any suggestion to do so in Kadansky. In addition, Kadansky fails to teach or suggest "wherein the second computer services the requests if the messages are valid and are received within a predetermined time interval," as required by claim 1. While the session moderator does send beacon messages to the clients in a session, the session moderator at no time sends a "request" of any kind to the clients. Thus the clients never service a request from the session moderator.

Another possible reading is to interpret "the computer" recited in claim 1 as a first client, and the "second computer" as a second client. However, under this reading, Kadansky fails to teach or suggest "establishing an authentication handshake with the second computer," as required by claim 1. The term "authentication handshake" is well-known and signifies some sort of mutual interaction performed between two devices, wherein each of the two devices identifies not only the other's identity, but also establishes the other's authority to transact. In Kadansky, at no time do two of the clients in the network perform an "authentication handshake." At best, one client simply sends a message, such as an email message, to another client, without any sort of mutual interaction to determine each other's identities or authorization. Accordingly, claim 1, together with its dependent claims (2-6) are patentable over the cited art. The dependent claims contain patentable limitations, also.

The arguments set forth above with respect to claim 1 apply equally to independent claims 7, 13, 19, 25, 29, 30, 33, 36, 39, 42, 43, 46, and 47. Accordingly, independent claims 7, 13, 19, 25, 29, 30, 33, 36, 39, 42, 43, 46, and 47, together with their respective dependent claims, are also patentable over the cited art. The dependent claims contain patentable limitations, as well.

III. New Claims

New claims 48-65 have been added. Support for the new claims is found in the specification at pages 10-18, for example.

New claims 48-65 are also patentable over Kadansky.

New independent claim 48 requires "receiving from a device verification information verifying the identity of the device," "verifying the validity of the verification information using common information known to the device and to the processor," and "determining an authorization status of the device based on (1) the validity of the verification information and (2) a time the verification information is received by the processor." New claim 48 additionally comprises "receiving a request from the device to access the stored data," and "allowing the device to access the stored data based, at least in part, on the authorization status at the time the request is received."

Nowhere does Kadansky teach or suggest "determining an authorization status of the device based on (1) the validity of the verification information and (2) the time the verification information is received by the processor," as required by claim 48. While Kadansky discloses determining whether or not to discard a message, Kadansky does not discuss determining an authorization status of a device. If a client in the network determines that a message is old, for example, that message will be discarded. However, the communication link between the client and the sender of the message will be maintained, and future messages continue to be examined. In the claimed invention, in contrast, if the storage server does not receive from the client valid verification information (which may be in the form of a heartbeat message, for example) during a particular interval, the client's authorization is immediately discontinued and future requests are not serviced. Nor does Kadansky teach or suggest "receiving a request from the device to access the stored data," as required by claim 48. Stored data is not discussed at all in the reference. Clearly, then, Kadansky also fails to teach or suggest "allowing the device to access the stored data based on the authorization status at the time the request is received," as also required by claim 48. Accordingly, new claim 48, together with its dependent claims (49-61) are patentable over Kadansky. The dependent claims also contain patentable limitations.

New independent claim 62 requires "providing authentication information to a processor responsible for managing data processing requests relating to stored data.". New claim 62 additionally requires performing, at least once during one or more time intervals having predetermined durations, the following actions: "retrieving from memory a value previously received from the processor," "applying a predetermined algorithm to the value to generate an encoded value," and "transmitting the encoded value to the processor." New claim 62 further requires “transmitting to the processor at least one data processing request relating to the stored data.”

Kadansky does not teach or suggest this combination of features. For example, Kadansky does not disclose a processor responsible for managing data processing requests relating to stored data, and thus fails to teach or suggest “providing authentication information to a processor responsible for managing data processing requests relating to stored data.” Accordingly, new claim 62, together with its dependent claims (62-66) are patentable over Kadansky. The dependent claims also contain patentable limitations.

New claim 67 is a system claim having limitations similar to those of new claim 48. Thus, for the reasons set forth above with respect to new claim 48, new claim 67 is also patentable over the cited art.

IV. Conclusion

In view of the foregoing, each of claims 1-67 is believed to be in condition for allowance. Accordingly, entry and reconsideration of these claims are respectfully requested.

Respectfully,

By
Jonathan Tyler
Attorney for Applicants
Reg. No. 52,308
212-836-8653

Date: September 30, 2005